BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

[Additional counsel listed on signature page]

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

In re InMarket Media Location Data Tracking Litigation

Case No. 3:24-cv-00511-JSC

SECOND CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Judge: Jacqueline Scott Corley

Plaintiffs Autry Willis and Kenneth Kruger ("Plaintiffs"), by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves, which are based on personal knowledge, against Defendant InMarket Media, LLC ("InMarket" or "Defendant").

NATURE OF THE ACTION

1. InMarket violates state law by acquiring and tracking consumers' precise geolocation data and other data without authorization, aggregating it with other data points, and then monetizing the data.

2. It does so through multiple channels.

3. One such channel is smartphone applications, including: (1) InMarket-owned and -operated applications and (2) use of spyware called "InMarket SDK" which is imbedded on numerous third-party applications

4. The data InMarket collects and uses can include consumers' private movements to and from sensitive locations, like locations associated with medical care, reproductive health, religious worship, mental health, rallies, demonstrations, or protests.

5. In addition to acquiring this private data without consumers' informed consent, InMarket fails to notify consumers that it then aggregates that location data with other data points to develop consumer profiles. Nor does InMarket notify consumers that this data will be used for targeted advertising. It does all of this without consumers' consent.

6. Plaintiffs are individuals who assert claims on behalf of themselves and class members for violations of California privacy statutes and unjust enrichment.

7. By selling this data without consent, Defendant has been unjustly enriched and has violated Plaintiffs' privacy rights, state consumer protection laws, and privacy statutes.

8. InMarket was investigated by the Federal Trade Commission (FTC) for this very conduct and was ultimately required to stop selling and licensing precise location data and to delete what it already obtained.

9. InMarket has not publicly disputed the FTC's allegations or findings. Rather, its CEO spoke approvingly of the process, characterizing the FTC's enforcement action as a partnership in which InMarket was "vetted by the FTC."

10. The FTC, however, characterized its enforcement actions against InMarket and other companies like it as addressing the "pervasive extraction and mishandling of consumers' sensitive personal data" that imposed "serious privacy threats."

PARTIES

11. **Plaintiff Autry Willis** is a resident of Oakland, California. Plaintiff Willis downloaded one or more phone applications which, upon information and belief, contained geolocation data tracking technology ("Apps").

12. On information and belief, the Apps used by Plaintiff Willis included:

(a) Pandora,[1] which Plaintiff used on approximately a daily basis from approximately 2017 to 2023, including in her workplace and home;

(b) CVS,[2] which Plaintiff downloaded in approximately 2021 and which she still has on her phone;

[1] *Pandora Adds InMarket to its Preferred Provider List; Will Leverage its Location Conversion Index (LCI) to Measure Advertising-Driven Store Visits*, PR Newswire (Mar. 3, 2021), https://www.prnewswire.com/news-releases/pandora-adds-inmarket-to-its-preferred-provider-list-will-leverage-its-location-conversion-index-lci-to-measure-advertising-driven-store-visits-301239504.html#:~:text=Pandora%20expects%20to%20use%20InMarket's%20LCI%20to,consumer%20intelligence%2C%20real%2Dtime%20activation%20and%20attribution%20for.

[2] Natalie Gagliordi, *How the quiet rise of beacons has reshaped retail marketing*, ZD NET (Feb. 13, 2016), https://www.zdnet.com/article/how-the-quite-rise-of-beacons-has-reshaped-retail-marketing/;

Marketing in the Face of a Pandemic, MMA Global (June 25, 2020), https://www.mmaglobal.com/files/webinars/inmarket_final.pdf;

Q4 2024 Xlear CVS Campaign, InMarket Live Campaigns (October 8, 2024), https://inmarket.com/creative/xlearclient-directq4-2024-xlear-cvs-campaignq4-2024/;

Apple App Store page for InMarket-owned App "Key Ring Rewards Card Wallet," noting ability to link accounts for, among others, CVS and Walmart; available at: https://apps.apple.com/us/app/key-ring-rewards-card-wallet/id372547556.

(c) Michaels,[3] which Plaintiff downloaded in approximately 2018 or 2019 and used for a period of time.

13. While she had these Apps on her phone, Plaintiff Willis routinely traveled with her phone to various locations—including her home, work, medical appointments, religious services, and other places she considers sensitive and private.

14. At the time Plaintiff Willis downloaded the Apps, she believed that the Apps would not transfer her geolocation data to another entity for the purposes of selling said data.

15. However, that was not the case: the Apps sent location data to Defendant when Plaintiff Willis used the Apps. During that entire time, the Apps tracked the geolocation of Plaintiff Willis. In turn, Defendant tracked Plaintiff Willis's geolocation in California, and then sold that data for profit. Plaintiff Willis suffered her primary injury in California.

16. During the time Plaintiff Willis used the Apps, Defendant took Plaintiff Willis's geolocation data from the App and then sold Plaintiff Willis's location data to other third parties.

17. Plaintiff Willis has not consented to have her geolocation data sold to third parties for valuable consideration. If Plaintiff Willis had been aware that Defendant would receive and sell her geolocation data to third parties, Plaintiff Willis would not have used the App.

18. **Plaintiff Kenneth Kruger** is a resident of Palo Alto, California. On information and belief, Plaintiff Kruger downloaded one or more Apps, including:

(a) CVS, which Plaintiff Kruger downloaded on and used after October 14, 2012, and which he still has on his phone, and

[3] *See, e.g., Back-to-School Lookback InSights, Informative InSights from the 2023 B2S Shopping Season*, InMarket (May 2024), https://2750857.fs1.hubspotusercontent-na1.net/hubfs/2750857/Reports_Whitepapers_Webinars/2024%20Back-to-School%20Lookback%20InSights.pdf.

(b) Walmart,[4] which Plaintiff Kruger downloaded on and used after September 16, 2013, and which he still has on his phone.

19. While he had these Apps on his phone, Plaintiff Kruger routinely traveled with his phone to various locations—including his home, work, medical appointments, church, and other places he considers sensitive and private.

20. At the time he downloaded his Apps, Plaintiff Kruger believed that the Apps would not transfer his geolocation data to another entity for the purposes of selling said data.

21. However, that was not the case: the Apps sent location data to Defendant when Plaintiff Kruger used the App. During that entire time, the Apps tracked the geolocation of Plaintiff Kruger. In turn, Defendant tracked Plaintiff Kruger's geolocation in California, and then sold that data for profit. Plaintiff Kruger suffered his primary injury in California.

22. During the time Plaintiff Kruger used the Apps, Defendant took Plaintiff Kruger's geolocation data from the Apps and then sold Plaintiff Kruger's location data to other third parties.

23. Plaintiff Kruger has not consented to have his geolocation data sold to third parties for valuable consideration. If Plaintiff Kruger had been aware that Defendant would receive and sell his geolocation data to third parties, Plaintiff Kruger would have not used the App.

24. **Defendant InMarket Media, LLC**, is a Delaware limited liability corporation with its principal place of business in Austin, Texas.

[4] *See, e.g., InMarket Insights: Walmart Tops in Customer Loyalty*, Homepage News (Feb. 16, 2022), https://www.homepagenews.com/retail-articles/inmarket-insights-walmart-tops-in-customer-loyalty/;

Apple App Store page for InMarket-owned App "Key Ring Rewards Card Wallet," noting ability to link accounts for, among others, CVS and Walmart; available at: https://apps.apple.com/us/app/key-ring-rewards-card-wallet/id372547556;

The Path to Purchase Institute adds inMarket Loyalty Data to its Retailer Profiles, Hospitality Technology (June 20, 2019), ("inMarket will be providing reports on loyalty and dwell time for more than 30 major retail chains in the U.S.., including Walmart…."; discussing "average dwell time per visit" and Walmart and other retailers) https://hospitalitytech.com/path-purchase-institute-adds-inmarket-loyalty-data-its-retailer-profiles.

25. InMarket obtains location data on more than 200 million active users each month[5] using "the world's most popular apps."[6]

26. The list of applications which have used the InMarket SDK or otherwise sent location data to InMarket is not public or available to Plaintiffs but is known to InMarket.

27. InMarket intentionally conceals its application list from the public.

28. The means through which InMarket obtains location data is further concealed by its use of third-party applications and data sources.

29. When the *The New York Times* analyzed location tracking companies in December 2018, it reported that Perfect365, an application which has used the InMarket SDK, "said it could not discuss any data practices because of nondisclosure agreements."

30. In 2018, Jennifer Valentino-DeVries, one of the "tech reporters on the *NY Times* Investigations team that uncovered how companies track and sell location data from smartphones," participated in an "Ask Me Anything" discussion on Reddit.[7]

31. Valentino-DeVries stated that she could not suggest a list of tracking applications to delete to protect consumer privacy because "in the course of reporting, we learned that many apps gather the data, get it on their servers and then sell it to other companies. We can't see that kind of sharing, can't test it, and can't learn about it unless the companies respond to us and acknowledge it."

32. In 2019, Charlie Wartzel and Stuart Thompson, authors of *The New York Times* feature "One Nation, Tracked," which "looked at the movements of 12 million Americans based on

[5] InMarket Home Page/Data, https://inmarket.com/data/ (last visited Dec. 17, 2024).

[6] *inMarket Launches Interactive Moments, a Powerful Location-Based Advertising Suite for Brands,* PR Newswire (Nov. 29, 2018), https://www.prnewswire.com/news-releases/inmarket-launches-interactive-moments-a-powerful-location-based-advertising-suite-for-brands-300757483.html.

[7] *I'm Jennifer Valentino-DeVries, a tech reporter on the NY Times investigations team that uncovered how companies track and sell location data from smartphones. Ask me anything.,* Reddit https://www.reddit.com/r/IAmA/comments/a7cnc0/im_jennifer_valentinodevries_a_tech_reporter_on/?sort=confidence (last visited Dec. 17, 2024).

phone location data," also participated in an "Ask Me Anything" discussion on Reddit.[8] They echoed Ms. Valentino-DeVries' findings:

> Naming specific apps is difficult because companies rarely disclose who they work with. Honestly, this is one of the most frustrating things with reporting on this industry. It's a real black box — even people who work in the weeds don't quite know where information is going . . . or where it's been.

33. Plaintiffs have numerous applications on their devices, in addition those identified above.

34. Given the ubiquity of InMarket's tracking, it is likely that a reasonable opportunity for further investigation and discovery will reveal evidentiary support for InMarket's tracking of Plaintiffs and their locations through numerous applications including and beyond those identified in this complaint.

JURISDICTION AND VENUE

35. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) because this is a class action in which at least one member of the class is a citizen of a state different from any Defendant, the amount in controversy exceeds $5 million, exclusive of interest and costs, and the proposed class contains more than 100 members.

36. This Court has personal jurisdiction over Defendant because a substantial portion of the events giving rise to this cause of action occurred here and Defendant otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in California. Plaintiffs are domiciled and suffered their primary injuries in this District.

37. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

---

[8] *We are Charlie Warzel and Stuart Thompson of The New York Times Opinion Section. Let's talk about our project, "One Nation, Tracked," looking at the movements of 12 million Americans based on phone location data. Ask us anything.*, Reddit https://www.reddit.com/r/IAmA/comments/edd7ns/we_are_charlie_warzel_and_stuart_thompson_of_the/ (last visited Dec. 17, 2024);

See also, e.g., Stuart A. Thompson and Charlie Warzel, *Smartphones Are Spies. Here's Whom They Report To.,* The New York Times (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html.

FACTUAL ALLEGATIONS

A. InMarket collects sensitive information from App users on over 300 million mobile devices.

38. InMarket is a digital marketing platform and data aggregator.

39. It collects consumer location data through applications InMarket owns and its software development kit (the InMarketSDK) incorporated into third-party mobile applications.

40. InMarket SDK is a collection of development tools that can be incorporated into a mobile application.

41. InMarket SDK's function is to collect the location data of all mobile application users who have InMarket SDK spyware embedded in their Apps, and transmit the consumer's precise location back to Defendant.

42. Thus, through the use of its spyware, InMarket monitors, tracks, and identifies consumers in real time, including Plaintiffs and other putative class members.

43. Defendant fails to notify consumers that their location data will be used for targeted advertising and fails to verify that Apps incorporating the InMarket SDK have notified consumers of such use.

44. Defendant incorporates InMarket SDK into more than 300 third-party Apps, which have been downloaded onto over 390 million unique devices since 2017.

45. Apps that incorporate the InMarket SDK request access to the location data generated by a mobile device's operating system.

46. Critically, the InMarket SDK receives the device's precise latitude and longitude, along with a timestamp and unique mobile device identifier, as often as the mobile device's operating system provides it— ranging from almost no collection when the device is idle, to every few seconds when the device is actively moving—and transmits it directly to Defendant's servers.

47. The FTC reported that, as a result, about 100 million unique devices have sent Defendant location data *each year* beginning in 2016.

48. InMarket's website claims it reaches more than 200 million active users *each month*, via first- and third-party sources verified "for accuracy & precision."[9]

49. Defendant collects sensitive information from consumers, including where they live, where they work, where they worship, where their children go to school or obtain child care, where they received medical treatment (potentially revealing the existence of medical conditions), whether they went to rallies, demonstrations, or protests (potentially revealing their political affiliations), and any other information that can be gleaned from tracking a person's day-to-day movements.

50. This information is collected with several identifiers (including a unique mobile device identifier). Defendant has retained this information for up to five years.

51. InMarket uses the consumer data to facilitate targeted advertising to consumers on their mobile devices for the company's clients, which include brands and advertising agencies. Defendant fails to notify consumers that their location data will be used for targeted advertising and fails to verify that apps incorporating the InMarket SDK have notified consumers of such use.

B. <u>InMarket touts the precision of its location tracking.</u>

52. InMarket's October 16, 2019 home page touted its "Hyper-Accurate SDK Derived Location Data":

> inMarket is the first company to commit to 100% Comscore verified, always on SDK data and the first to advocate for location transparency via 3rd party measurement. One of the largest of it's [sic] kind, this network comprises hundreds of the world's most popular apps and 50 million active 1st party SDK connections as verified by Comscore.[10]

53. InMarket's November 1, 2020 page boasted the "InMarket Difference" of tracking "consumers on the move":[11]

> **SDK derived, always-on location data**
> Our Moments SDK is always-on to leverage GPS and indoor

[9] InMarket Home Page/Data, https://inmarket.com/data/ (last visited Dec. 17, 2024).

[10] Internet Archive Wayback Machine inMarket webpage from Oct. 16, 2019, available at: https://web.archive.org/web/20191016011044/https://inmarket.com/#inmarket-difference.

[11] Internet Archive Wayback Machine inMarket webpage from Nov. 1, 2020, available at: https://web.archive.org/web/20201101010459/http://inmarket.com/.

> location signals while consumers are on the move, providing the most accurate and precise delivery of Lat/Long, POI, time, date and dwell time of a visit available today.[12]
>
> **Transformational measurement, deep consumer intelligence & unrivaled flexibility**
> Reveal who your customers truly are. Learn what they buy, where they go, when they're most receptive to brand engagement, and what truly motivates them. Solutions available as a managed service via data feeds (DaaS) or dashboards (SaaS).

54. "Always on" is as it sounds: it means the app is "always on," running in the background, even when the user is not actively using the app or is offline entirely.

55. InMarket's location-tracking SDK is in Apps used for grocery stores, quizzes, games, beauty, sports, entertainment, and more.

56. Roam.ia, another location tracking company, explains always-on location SDKs,[13] noting:

> Each SDK will have different capabilities depending on who is supplying it. Some combine and process data from multiple sources to increase the accuracy and precision of native location data. Others are designed to be "always-on"", even when the user is offline or the app is running in the background. And some are built specifically to process data into detailed location intelligence of the user's movements for marketing or ad campaigns.

57. InMarket's SDK has all of those capabilities.

58. In addition, InMarket has specifically developed technology to overcome privacy protections. In March 2021, it published a whitepaper called "Crumbling Cookies: The Demise of Third-Party Cookies and the Rise of Geo-Contextual, Real-Time Marketing,"[14] discussing the "death of the cookie" as "greater privacy concerns have led to better privacy safeguards."

---

[12] *See also, e.g. Internet* Archive Wayback Machine inMarket webpage from Sept. 27, 2021, available at https://web.archive.org/web/20210927214914/https://inmarket.com/ (substantially similar language from Sept. 21, 2021).

[13] Marc Kranendonk, *What is a location SDK? A Complete Guide for 2024*, Roam.ai (Jan. 30, 2024), https://www.roam.ai/blog/what-is-a-location-sdk.

[14] *Crumbling Cookies: The Demise of Third-Party Cookies and the Rise of Geo-Contextual, Real-Time Marketing*, InMarket (March 2021), https://f.hubspotusercontent00.net/hubfs/2750857/Reports_Whitepapers_Webinars/InMarket%20InSights%20Crumbling%20Cookies.pdf.

59. In that paper, InMarket discussed how it combatted privacy safeguards. It explained how it intentionally overcame bans on third-party tracking by integrating itself with "partners [who] are classified as a first-party cookie on those sites and not a third-party cookie."

60. InMarket used this technology to link data from desktop devices with data from mobile devices, including location data:

> When InMarket's measurement pixel fires upon exposure, it sends our cross-device partner's first party cookie, and therefore it is unaffected by Google's ban. In addition, this also allows desktop exposure to be mapped to mobile devices, which LCI® can then use to measure foot traffic. These processes, already adopted by InMarket, will actually become the industry standard when third-party cookies are removed entirely.

61. InMarket noted that the average American has numerous connected devices in their own homes. And "people- and household-based advertising can . . . deduce[a user] down to an individual personal or household," noting that "[t]he rise of IDs that revolve around consumers and the household, are behaviors-based, and use real-time data will allow marketers to reach consumers at their precise moment of need, regardless of device or channel."

62. InMarket uses an "InMarket ID, and other contextual ad targeting" as well as "its own household graph" and the use of "cross-device partners" to track users as they switch devices and move from desktop traffic to mobile traffic to foot traffic. InMarket uses this technology to overcome bans or privacy settings prohibiting third-party cookies, because the partners who integrate its technology are treated as first parties.

63. A household graph maps a household's connected devices into household or use profiles to be targeted—e.g., phones, tablets, computers, and smart TVs.

64. InMarket recently announced a new partnership with TikTok—a company whose tracking capabilities are so precise and invasive that both the Trump and Biden administrations have sought to ban the app from the country as a national security risk.

65. The new partnership highlights the depth and precision of InMarket's tracking. InMarket can, for example, track if a TikTok user saw a product in a particular TikTok user's video and then went to the physical store to purchase it.

66. InMarket tracks users as they travel from one location to another, with a level of granularity down to the aisle where they shop.

C. InMarket's patents further reveal its invasive tracking capabilities.

67. The precise tracking capabilities of InMarket are expressly stated in their patent filings.

68. For instance, under patent number US-10779109-B2, InMarket currently has the ability to accurately and precisely track consumers' location behavior change in response to ads they are exposed to. As explained in detail in the patent filing, InMarket can effectuate this capability by "creat[ing] two groups of consumers with substantially similar "attribute data including demographic data (e.g., data indicating that the user is female, 30-40 years old, resides in San Francisco, Calif., has a household income of $100,000, etc.), behavioral data (e.g. the user visits a coffee shop three times per week), third party data (e.g., purchased a condo for $200,000 in 2006), psycho-graphic data (e.g. leads a healthy lifestyle, likely to vote for a particular political party, etc.), and other attribute data, track their location behavior and measure the influence of ads on their location behavior by identifying anomalies in visitation patterns, i.e. location behavior, in one group that was exposed to a particular ad in comparison to the control group that was not."

69. Another patent filing, US-10149094-B2, describes InMarket's methods for determining the coordinates of a mobile device's location using a location determination system, such as a global positioning system. InMarket's database stores the identifiers of cells representative of predefined regions in a hierarchical grid system which is constructed in a longitude latitude space of location coordinates, with resolution levels aligned with decimal precision levels of the location coordinates.

70. Strikingly, InMarket's capabilities go beyond accurate and precise tracking of geolocation data. As evidenced in detail in filings under patent number US-20150358818-A1, InMarket has the capability to turn mobile devices it tracks into surveillance gadgets to spy on and communicate with other consumers in the same store. In other terms, InMarket's technology allows for not only the collection of transaction and geo-location data but also the dissemination of

information, in the form of coupons, marketing advertisements, among others, to mobile devices of unsuspecting consumers by using mobile phones with InMarket SDK. The patent filing elaborates on the technology: "a software application program (app) executing with the computing environment of a mobile device is used to configure the mobile device to sense trigger events, communicate with a wide area network, generate or receive information or value signals, implement various security protocols, and forward the information and value signals to other proximate mobile devices."

71. A real use example is where "a consumer entering a store and encountering one or more signals could have their device ID tagged with information on the stores visited, areas browsed, time spent, and/or products they were interested in. This information may be stored at a location locally, on a mobile device, and/or on a server."

72. Furthermore, once a consumer is caught up in the cobweb of InMarket's tracking system, they can be targeted with advertisements and messages "beginning before and/or stretching after the mobile device has left the location." This, as the patent admits, represents the application of online retargeting (practice of identifying a consumer who visited a certain webpage and messaging the same consumer with an ad about the first webpage at a later time, on a different website) into another dimension, real and physical world.

D. Location tracking like InMarket's is invasive.

73. In December 2018, *The New York Times* published an article entitled, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret."[15] The article discussed how even supposedly anonymized location tracking can reveal individual identity through, for example, a consumer's work commute or time spent regularly at a home address. The article discussed how such tracking applications gather private information, noting one woman's concerns about tracking of her visit for medical procedure, a Weight Watchers meeting, and a stay at an ex-boyfriend's home. The article noted that "explanations people see when prompted to give

[15] Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, The New York Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

permission are often incomplete or misleading" and do "not mention that the data will be shared and sold."

74. As *The New York Times* reported in a September 2020 article entitled, "How Mobile Phones Became a Privacy Battleground—and How to Protect Yourself," phone users do not understand that their data is being tracked[16]:

> [I]t [is] nearly impossible for phone owners to track where their data goes or how it gets used, let alone prevent that data from being shared in the first place. . . . [T]he industry has no standards to follow, so it's difficult for everyone to figure out what is and isn't possible on any given device. What phone owners have instead are sometimes-complicated menus full of permissions that are buried deep within an operating system and rarely set up by default with their privacy in mind.

75. The article quotes an in-house privacy attorney and data-protection officer discussing her fears about companies using SDKs the way InMarket does:

> Whitney Merrill, a privacy attorney and data-protection officer, told us that what scares her most "are the SDKs and random packages that people are throwing in that still collect data in ways that weren't anticipated." Merrill described a hypothetical—though not unlikely—scenario in which an app developer monetizes its app by putting in a bunch of different advertising SDKs to leverage as many networks as possible. But because the developer hasn't investigated the privacy practices of those ad networks, those SDKs could take all the data that passes through them when you use the app, package that data up, and then sell it; these entities could continue to pass your data along, combining it with data from other companies until it forms a clear picture of your behavior. This data can be bought and sold for advertising purposes, or purchased by agencies of the US government.

76. A private investigator was able to obtain consumer data from another data broker like InMarket: Babel Street. Like InMarket's technology, Babel Street's Local X "tool relies on the mobile advertising ID that Google and Apple assign to each phone to serve users targeted ads. Advertisers can then build a growing profile of information around that ID based on where it accesses services that deliver ads."[17]

---

[16] Thorin Klosowski, *How Mobile Phones Became a Privacy Battleground-and How to Protect Yourself*, The New York Times Wirecutter (Sept. 29, 2022), https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/.

[17] Emma Roth, *An investigation exposes data brokers using ads to help track almost any phone*, The Verge (Oct. 23, 2024), https://www.theverge.com/2024/10/23/24277679/atlas-privacy-babel-street-data-brokers-locate-x-tracking.

77. But the nature of such tracking means that individuals are followed well beyond their shopping trip, actively tracking their whereabouts, including the most private moments of their lives:

> [T]he data . . . allowed a reporter to zoom in on the parking lot of an abortion clinic in Florida and observe more than 700 red dots, each representing a phone that had recently visited the clinic. Location X then allowed the reporter to trace the movements of one specific device.
>
> That device—and by extension, the person carrying it—began the journey in mid-June from a residence in Alabama. The person passed by a Lowe's Home Improvement store, drove on a highway, visited a church, crossed into Florida, and finally stopped at the clinic where the phone indicates the person stayed for two hours before leaving and returning to Alabama. The data tracked the phone as having visited the clinic only once.[18]

78. One advertising group previously used location data to target "abortion-minded" women with anti-choice advertising.[19]

79. While details about InMarket's data cache remain opaque and in its sole possession, InMarket undoubtedly collected consumers' precise, minute movements, to private locations, unrelated to any consented-to services.

80. Indeed, in December 2023, InMarket announced that it had been working with a nonprofit "for the past year" "to identify location data near reproductive health facilities and remove it from the InMarket database."[20]

---

[18] Dan Goodin, *Location Tracking of phones is out of control. Here's how to fight back.*, Ars Technica (Oct. 23, 2024), https://arstechnica.com/information-technology/2024/10/phone-tracking-tool-lets-government-agencies-follow-your-every-move/.

[19] Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, Rewire News Group (May 25, 2016), https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/.

[20] *InMarket Partners with Power to Decide to Protect Reproductive Care Location Privacy; Create New Model for Nonprofit and Industry Collaboration*, PR Newswire (Dec. 19, 2023), https://www.prnewswire.com/news-releases/inmarket-partners-with-power-to-decide-to-protect-reproductive-care-location-privacy-create-new-model-for-nonprofit-and-industry-collaboration-302018808.html?tc.

81. InMarket acknowledged a "technical challenge in fully removing potentially sensitive data because there was no clearinghouse to identify these locations for blocking and removal."

82. Despite claiming to have "policies against targeting sensitive locations, including the offices of reproductive and sexual health providers," as well as "K-12 schools, military institutions, abuse shelters, houses of worship, and LGBTQ-focused places," InMarket conceded having collected this data anyway.

83. Only after the FTC began challenging InMarket's conduct did InMarket—an amply resourced multimillion dollar company—engage a nonprofit to attempt to "purge any reproductive care visit data from its systems" and help "identify all locations to be removed."

E. Defendant monetizes users' location data through targeted advertising.

84. Defendant sorts consumers based on their visits to points of interest into audience segments to which it can target advertising.

85. Defendant has created or maintains almost two thousand distinct advertising audience segments.

86. For example, an InMarket brand client can target shoppers who are likely to be low-income millennials; well-off suburban moms; parents of preschoolers, high-school students, or kids who are home-schooled; Christian church goers; convenience-sensitive or price-sensitive; single parents or empty-nesters; affluent savers or blue collar workers; "healthy or wealthy" or "wealthy and not healthy," to name only a selection of the categories InMarket offers or has offered to its brand clients.

87. InMarket classifies audiences based on both past behavior and predictions it makes about consumers based on that behavior.

88. For example, if a consumer's past location data shows that she has visited a car dealership, InMarket can combine that information with the consumer's attributes purchased from other sources (age, income, family structure, education level), and can potentially predict that she may be in the market for a certain type of vehicle.

89. The InMarket SDK displays the ads and determines which ads appear in which apps incorporating the SDK.

90. Defendant additionally offers advertisers a product that sends push notifications based on a consumer's location and "geofencing," the creation of a virtual fence around a particular point of interest. When the InMarket SDK transmits a location that is inside a virtual fence, the app will send a push notification for a particular ad.

91. For example, a consumer who is within 200 meters of a pharmacy might see an ad for toothpaste, cold medicine, or some other product sold at that location.

92. Finally, Defendant also makes its advertising audience segments available on real-time bidding platforms. An advertiser using one of these platforms can select an advertising audience and identify the amount that it is willing to pay (that is, its bid) each time its ad appears on a mobile device that is a part of that audience.

93. The advertiser's ad will appear on a particular device if it has the highest bid for that device.

94. Defendant receives revenue each time an advertiser uses one of its audiences in this process.

95. In addition to incorporation of the InMarket SDK into third-party apps, Defendant has incorporated the InMarket SDK into mobile applications that it owns and operates ("InMarket Apps"). InMarket Apps consist of applications InMarket created soon after the company's formation and mobile applications it acquired as part of a campaign to expand its reach and location database. The former applications include CheckPoints, which offers shopping rewards for completing tasks such as watching videos and taking online quizzes, and ListEase, which helps consumers create shopping lists. These applications have been downloaded onto over 30 million unique devices since 2017.

96. Since 2010, InMarket has offered the CheckPoints app on both the iOS and Android platforms. InMarket's CheckPoints app is marketed as a "rewards app," and promises users "easy money—earn as you shop." It tells consumers to "join the millions earning free gift cards and more every day." Users of the app collect points by performing various tasks (checking into retail

locations, watching videos, scanning certain products while in store, taking surveys and quizzes), and then exchange those points for rewards, such as gift cards. The app is free to download and includes in-app advertising.

97. Since 2012, InMarket has offered the ListEase app on both the iOS and Android platforms. The ListEase app markets itself as an electronic shopping list app. The app is free to download and includes in-app advertising.

98. The consent screens used for both the CheckPoints and ListEase apps tell consumers that their location will be used for the app's functionality (earning points and keeping lists), which are misleading half-truths. Thus, users are choosing to share their location with these apps for specific purposes completely unrelated to InMarket's larger advertising-related business.

99. At no point during the consent process for either the CheckPoints or ListEase apps did InMarket also disclose that it was collecting users' precise location, often multiple times per hour, along with data collected from multiple other sources—including through Apps using the InMarket SDK—to build extensive profiles on users to be used to precisely target them with advertising.

100. Although InMarket discloses in its privacy policy that it uses consumer data for targeted advertising, its consent screen does not link to the privacy policy language, and the prompts do not inform consumers of the apps' data collection and use practices.

101. In her investigation, tech reporter Valentino-DeVries learned that location tracking disclosures were confusing and incomplete, when made at all:

> What we found when we tested apps was that they ask users for permission to obtain their location data, but in doing so they typically provide an incomplete explanation of how the information will be used. For example, they will say something like "This app would like to access your location. We will use this to provide you with more customized weather alerts," or with traffic updates, or what have you. They usually do not mention advertising, and almost none mention sale or retention of the data beyond advertising.
>
> The other uses may be mentioned in a privacy policy, but it was difficult even for us to tell for certain. Companies we knew were funneling data for use by financial services firms, for instance, used vague phrases such as those saying the data could also be used for "business purposes."

> So, to understand the scope of the sharing, as a user, you would have to recognize that the initial message was incomplete, navigate to the privacy policy, read the entire thing and figure what phrases such as "business purposes" or "analysis of traffic patterns" actually mean.

F. InMarket has acquired numerous tracking companies to expand its location-data reach.

102. In 2019, InMarket launched a campaign of mobile application acquisitions to expand its consumer reach and location database.

103. To that end, in August 2019, InMarket announced the acquisition of Thinknear, a location-based mobile marketing platform.

104. The Thinknear acquisition was significant—doubling the headcount and revenue of InMarket. Telenav offered connected car and location-based services, i.e., it can track where consumers drive and serve advertising to them in their vehicles.[21]

105. InMarket's press release on the acquisition described the benefit of the partnership with the following words:

> The acquisition will allow Thinknear's clients to engage at the moment of truth through InMarket's 50 million Comscore-verified smartphone integrations. These direct connections enable brands to identify and engage consumers during multiple touchpoints of the purchase journey, including as they walk into any location in the US. InMarket's Moments technology delivers real-time, premium engagements with customers at precise locations during consideration and decision. InMarket clients will gain access to Thinknear's place-based targeting and Geotype technology, which create valuable high-performing profiles around ideal customers based on location behavior. Thinknear's Geolink is an advanced self-serve dashboard that will give InMarket clients one of their most requested features-- the hands-on ability to launch campaigns themselves from trading desks.[22]

106. Another press release also reported how the companies would partner to track where consumers drive:

---

[21] Chuck Martin, *InMarket Acquires Thinknear In Boost To In-Car Advertising*, MediaPost (Aug. 9, 2019), https://web.archive.org/web/20201029230812mp_/https://www.mediapost.com/publications/article/339084/inmarket-acquires-thinknear-in-boost-to-in-car-adv.html?edition=114905.

[22] *inMarket to Acquire Thinknear, Expand Location-Based Marketing Solutions*, PR Newswire (Aug. 8, 2019), https://www.prnewswire.com/news-releases/inmarket-to-acquire-thinknear-expand-location-based-marketing-solutions-300899051.html.

> Combining Telenav's Thinknear business with inMarket will create one of the largest location marketing technology providers in the country, with a broad reach of clients across the automotive, quick-service restaurant, retail and consumer packaged-goods industries, and a well-positioned innovator in the emerging connected-car media space.
>
> Following the closing of the transaction, Telenav plans to work with inMarket to offer unique in-car advertising to consumers via automotive manufacturers. Telenav's automotive expertise combined with inMarket's advertising and content delivery technologies will enable location-specific offers to be delivered to drivers who arrive in the parking lot of virtually any major big-box retailer in the United States. No other connected-car technology company has deployed such capabilities.[23]

107. In September 2020, InMarket announced the acquisition of assets from NinthDecimal, another location-based attribution and analytics company. The press release noted that "[m]arketers will now have access to an omnichannel platform that includes location and transactional audiences; GeoLink self-service marketing with real-time Moments; Location Conversion Index (LCI) attribution; and a robust set of advanced analytics -- all via one partner."[24]

108. NinthDecimal had previously acquired moLOGIQ in 2017[25] and Kiip in 2019[26].

---

[23] *Telenav Accelerates It's Connected-Car Media Strategy Through Strategic Transaction With Location-Based Marketing Leader InMarket*, Telenav Inc. (Aug. 8, 2019), https://www.telenav.com/press-releases/2019-08-08-telenav-accelerates-its-connected-car-media-strategy-through-strategic-transaction-with-location-based-marketing-leader-inmarket.

[24] *InMarket Acquires Assets from NinthDecimal, Creating the Definitive Leader in Real-Time, Data-Driven Marketing*, PR Newswire (Sept. 9, 2020), https://www.prnewswire.com/news-releases/inmarket-acquires-assets-from-ninthdecimal-creating-the-definitive-leader-in-real-time-data-driven-marketing-301126032.html.

[25] *NinthDecimal's Omni-Channel Marketing Platform Generates More Than 100 Percent Annual Revenue Growth for the Third Consecutive Year*, Globe Newswire (Mar. 15, 2018), https://rss.globenewswire.com/news-release/2018/03/15/1437926/0/en/NinthDecimal-s-Omni-Channel-Marketing-Platform-Generates-More-Than-100-Percent-Annual-Revenue-Growth-for-the-Third-Consecutive-Year.html;

NinthDecimal Acquires MoLOGIQ to Propel the Development of Location Intelligence Solutions, Globe Newswire (June 29, 2017), https://www.globenewswire.com/en/news-release/2017/06/29/1264362/0/en/NinthDecimal-Acquires-MoLOGIQ-to-Propel-the-Development-of-Location-Intelligence-Solutions.html.

[26] Edison Fu, *NinthDecimal gets Kiip in acquisition deal*, Global Corporate Venturing (Sep. 10, 2020), https://globalventuring.com/ninthdecimal-gets-kiip-in-acquisition-deal/;

Leo Kangin, *Kiip Co-Founder Brian Wong: 'I didn't even know that I wanted to be in the ad space'*, Brief Communications Inc. (Oct. 23, 2019), https://gobrief.com/interviews/kiip-with-brian-wong.

109. MoLOGIQ used SDKs and other technology and data—including demographic data and voter registration data—to process "billions of data signals." At the time of the NinthDecimal acquisition, MoLOGIQ's SDKs were on more than 50 million unique devices. MoLOGIQ had "successfully mapped 60 million devices to household addresses" allowing both "online and offline data sets" to be bridged.

110. Kiip was a mobile advertising network. It was sued in 2016 "for secretly tracking cellphone users' private information without those users' consent."[27] The case alleged that Kiip violated federal and state wiretapping laws by using in-app trackers to collect "consumers' personally identifying information, their current geographic location, and their individual cellphone device identifiers." That case later settled on a class-wide basis in state court.

111. Apps with the Kiip tracker include, for example, Zombie Assault, LGBT+, Think Dirty, Bullet Journal, Talking German Translator/Dictionary, and SkyVPN.[28]

112. In December 2020, InMarket completed the acquisition of Key Ring, the shopper loyalty app from Vericast.

113. InMarket advertised the acquisition as a further step to "empower brands to reach highly engaged, opted-in shoppers in real-time, while closing the loop on measuring campaign effectiveness," as well as "underscore[] the growing importance of first party data from opted-in consumers, and the value of real-time contextual advertising."[29]

114. In June 2021, InMarket acquired Out of Milk, a shopping list app with millions of downloads. InMarket announced this acquisition as a move to "further bolster its industry-leading suite of owned-and-operated apps, including ListEase, CheckPoints, and Key Ring, that span the journey as shoppers plan, save, and organize. These unique properties are part of InMarket's competitive advantage reaching shoppers across all stores and categories. The apps empower

[27] *Vasil, et al v. Kiip, Inc.,* 1:2016-cv-09937 (N.D. Ill.), ECF No. 1.

[28] Exodus tracker profile for Kiip, https://reports.exodus-privacy.eu.org/en/trackers/214/ (last visited Dec. 17, 2024).

[29] *InMarket Acquires Key Ring, Expanding its Data-Driven Marketing and Insights* Suite, PR Newswire (Dec. 10, 2020), https://www.prnewswire.com/news-releases/inmarket-acquires-key-ring-expanding-its-data-driven-marketing-and-insights-suite-301190647.html.

brands to reach a variety of highly engaged, opted-in shoppers in real-time."[30] Todd Dipaola, CEO and Founder of InMarket, highlighted the key function of this and the preceding acquisitions: to "scale InMarket" and its breadth of location data.

G. Defendant fails to verify that users of third-party apps incorporating InMarket's SDK have been notified that their location data will be used to target advertising.

115. Defendant does little to verify that third-party Apps obtain informed consumer consent before those third-party apps grant InMarket access to consumers' sensitive location data.

116. In fact, InMarket does not require third-party Apps to obtain informed consumer consent at all.

117. InMarket additionally neither collects nor retains records of any disclosures that third-party Apps do provide consumers before accessing their location data.

118. Even if these third-party App developers wanted to provide adequate disclosure to their users about InMarket's use of their location data, InMarket does not provide the developers with sufficient information to provide that notice.

119. Specifically, InMarket's contract with third-party App developers merely states that InMarket will serve ads on the developer's Apps in return for developers passing user information to InMarket, including precise location and advertising identifiers.

120. Defendant does not disclose that information collected from these third-party users will be supplemented and cross-referenced with purchased data and analyzed to draw inferences about those users for marketing purposes.

121. Defendant therefore does not know whether users of hundreds of third-party Apps were informed of their data being collected and used for targeted advertising.

[30] *InMarket Acquires Out of Milk to Bolster Real-Time, Contextual Advertising from Planning to Purchase*, PR Newswire (Jun. 22, 2021), https://www.prnewswire.com/news-releases/inmarket-acquires-out-of-milk-to-bolster-real-time-contextual-advertising-from-planning-to-purchase-301317186.html.

H. Defendant's practices cause and are likely to cause substantial injury to consumers.

122. Because Defendant combined consumers' location data with other personal information in its databases and systems without confirming user consent, Defendant obtained and used that data without informed user consent, resulting in consumer injury.

123. In addition, after collecting sensitive, precise location data about consumers' daily movements, Defendant retains that information longer than reasonably necessary to accomplish the purpose for which that information was collected and thereby exposes consumers to significant unnecessary risk. Specifically, InMarket has retained consumer location data for five years prior to deletion.

124. This unreasonably long retention period significantly increases the risk that this sensitive data could be disclosed, misused, and linked back to the consumer, thereby exposing sensitive information about that consumer's life.

125. Defendant's comprehensive collection and long-term retention of location data subjects consumers to a likelihood of substantial injury through the exposure of their re-identified location.

FTC'S JANUARY 2023 COMPLAINT AGAINST DEFENDANT

126. In January 2023, the FTC took action against Defendant for allegations that are substantially identical to this complaint.[31]

127. According to the FTC's complaint, Defendant's acts as described above constitute a violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce."

128. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

[31] FTC Complaint, https://www.ftc.gov/system/files/ftc_gov/pdf/Complaint-InMarketMediaLLC.pdf (last visited Dec. 17, 2024).

129. In January 2024, InMarket entered into a proposed settlement with the FTC.[32]

130. In April 2024, the FTC issued a Decision and Order following a Consent Agreement with InMarket.[33]

131. And in May 2024, the FTC announced that the settlement was finalized.[34]

132. The Consent Order and its mandates make clear that InMarket tracked personally identifiable, sensitive, precise geolocation data—without consumer consent—for purposes unnecessary to its business.

133. For example, the Consent Order banned InMarket from continuing to sell or license precise location data.

134. As another example, the Consent Order reflects that InMarket unlawfully required identifiable, sensitive information without consent. It required InMarket to delete the data it had already collected unless it (a) obtained consumer consent and (b) deidentified or otherwise rendered it non-sensitive.

135. InMarket publicly reframed the FTC's action as a partnership involving the FTC's due diligence into InMarket's business. It reported that the Consent Order followed *four years* of inquiry into InMarket by the FTC, after which InMarket's CEO stated: "It's like we've been vetted by the FTC."[35]

---

[32] *FTC Order Will Ban InMarket from Selling Precise Consumer Location Data*, Federal Trade Commission (Jan. 18, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-will-ban-inmarket-selling-precise-consumer-location-data.

[33] FTC Decision and Order, https://www.ftc.gov/system/files/ftc_gov/pdf/InMarketMedia-DecisionandOrder.pdf (last visited Dec. 17, 2024);

Consent Agreement, https://www.ftc.gov/system/files/ftc_gov/pdf/ACCO-InMarketMedialLLC.pdf (last visited Dec. 17, 2024).

[34] *FTC Finalizes Order with InMarket Prohibiting It from Selling or Sharing Precise Location Data*, Federal Trade Commission (May 1, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-finalizes-order-inmarket-prohibiting-it-selling-or-sharing-precise-location-data.

[35] Allison Schiff, *InMarket Acquires MMM Startup ChannelMix (And Says Its Tech Is Up To Code After Settling With The FTC)*, AdExchanger (Aug. 5, 2024), https://www.adexchanger.com/omnichannel-2/inmarket-acquires-mmm-startup-channelmix-and-says-that-its-tech-is-up-to-code-after-settling-with-the-ftc/.

136. InMarket's CEO spoke about the FTC's enforcement action as if it was an open and mutually beneficially partnership to improve industry standards, stating: "The work we did with the FTC over four years has helped create a blueprint for the industry and provide clarity about consumer consent and sensitive locations."

137. On March 5, 2024, however, the FTC published a blog post entitled "FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket."[36]

138. In the post, the FTC noticed "[t]here recent FTC enforcement actions," including its action against InMarket," "reflect a heightened focus on pervasive extraction and mishandling of consumers' sensitive personal data."

139. The FTC noted "common themes that highlighted serious privacy threats imposed on consumers by business models that monetize people's personal information" and made certain overarching pronouncements regarding the data privacy implications. For example:

> Browsing and location data paint an intimate picture of a person's life, including their religious affiliations, health and medical conditions, financial status, and sexual orientation.
>
> * * *
>
> Browsing and location data are sensitive. Full stop.
>
> * * *
>
> People have no way to object to—let alone control—how their data is collected, retained, used, and disclosed when these practices are hidden from them.

140. On December 4, 2024, the FTC published another blog posting that referenced its action against InMarket. The post, titled "Protecting consumers' location data: Key takeaways from four recent cases," talked about how location tracking information is inherently sensitive and, when associated with an identifier as InMarket does, is personally identifiable:

> **Location data is sensitive personal information.** In all four complaints [including the one against InMarket], the FTC says data aggregators collected billions of location data points linked to unique persistent identifiers and timestamps that could offer insights

[36] *FTC Cracks Down on Mass Data Collectors: A Closer Look at Avast, X-Mode, and InMarket*, Federal Trade Commission (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket.

> into people's movements. Unique persistent identifiers make it easy to match someone's movements with other personally identifiable information (PII) — like their name, address, or email address — from publicly available materials or other data brokers. Location data is sensitive personal information. Given the sensitivity, if you collect or sell it, you must protect it carefully.

CLASS ALLEGATIONS

141. ***Class Definition.*** Plaintiffs bring this action on behalf of a class of similarly situated individuals, defined as:

> All persons who reside in California whose data, including but not limited to their geolocation data, was collected by Defendant without their consent.

(the "Class").

142. Excluded from the Class are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, and members of the judge's staff, and the judge's immediate family.

143. Subject to additional information obtained through discovery, the foregoing class definition may be modified or narrowed by an amended complaint, or at class certification, including through the use of multi-state subclasses to account for material differences in state law, if any.

144. ***Numerosity.*** Members of the Class ("Class Members") are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the millions. The precise number of Class Members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

145. ***Commonality and Predominance.*** Common questions of law and fact exist as to all Class Members and predominate over questions affecting only individual Class Members. Common legal and factual questions include but are not limited to:

(a) Whether Defendant's sale of geolocation data without consent constitutes unjust enrichment;

(b) Whether Defendant engaged in the wrongful conduct alleged herein;

(c) Whether Defendant's collection, storage, distribution, and/or use of Plaintiffs' and Class Members' Personal Information violated privacy rights and invaded Plaintiffs' and Class Members' privacy; and

(d) Whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

146. ***Typicality.*** The claims of the named Plaintiffs are typical of the claims of the Class in that the named Plaintiffs' data was sold by Defendant without their consent, and the named Plaintiffs suffered injury as a result of Defendant's conduct.

147. ***Adequacy.*** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

148. ***Superiority.*** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class Members. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I
Invasion of Privacy

149. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

150. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

151. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

152. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest . . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. And Amends. To Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th 1, 81, (Mosk, J., dissenting).

153. Plaintiffs and the Class Members have a legally protected privacy interest, as recognized by the California Constitution, CIPA, common law, and the 4th Amendment to the United States Constitution.

154. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state privacy laws. Plaintiffs and Class Members were not aware and could not have reasonably expected that unknown third party would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiffs' and Class Members' sensitive information with other parties.

155. Defendant's conduct violates, at a minimum:

(a) The right to privacy in data, communications and personal information contained on personal devices;

(b) The California Constitution, Article I, Section 1;

(c) The California Wiretapping Act;

(d) The California Invasion of Privacy Act; and

(e) The California Computer Data Access and Fraud Act.

156. Defendant's conduct in secretly intercepting and collecting Plaintiffs' and Class Members' personal information, location data, and communications is an egregious breach of social norms and is highly offensive to a reasonable person.

157. Defendant's conduct in analyzing, using, and sharing with third parties the personal information and communications that Defendant intercepted and took from Plaintiffs' and Class Members is an egregious breach of societal norms and is highly offensive to a reasonable person, and violates Plaintiffs' and Class Members' reasonable expectations of privacy.

158. Plaintiffs and Class Members did not consent for Defendant to track, collect, or use their personal information and communications.

159. As a direct and proximate result of Defendant's invasion of their privacy, Plaintiffs and Class Members were injured and suffered damages. Plaintiffs and Class Members are entitled to equitable relief and just compensation in an amount to be determined at trial.

160. Defendant was unjustly enriched as a result of its invasion of Plaintiffs' and Class Members' privacy.

COUNT II

Violation of the California Computer Data Access and Fraud Act
Cal. Penal Code. § 502

161. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

162. The California legislature enacted the CDAFA with the intent of "expand[ing] the degree of protection afforded to individuals … from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code §502(a). The enactment of CDAFA was motivated by the finding that "the proliferation of computer

technology has resulted in a concomitant proliferation of … unauthorized access to computers, computer systems, and computer data." *Id.*

163. Plaintiffs' and Class Members' smartphones constitute "computers" within the scope of the CDAFA.

164. Defendant violated the following sections of the CDAFA:

(a) Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission . . . use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

(b) Section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;"

(c) Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

165. Defendant knowingly accessed Plaintiffs' and Class Members' smartphones without their permission by including within the SDK that Defendant provides to developers, software that intercepts and transmits data, communications, and personal information concerning Plaintiffs and Class Members.

166. Defendant used data, communications, and personal information that it intercepted and took from Plaintiffs' and Class Members' smartphones to wrongfully and unjustly enrich itself at the expense of Plaintiffs and Class Members.

167. Defendant took, copied, intercepted, and made use of data, communications, and personal information from Plaintiffs' and Class Members' smartphones.

168. Defendant knowingly and without Plaintiffs' and Class Members' permission accessed or caused to be accessed their smartphones by installing—without Plaintiffs' and Class

Members' informed consent—software that intercepts and/or takes data, communications, and personal information concerning Plaintiffs and Class Members.

169. Plaintiffs and Class Members are residents of California and used their smartphones in California. Defendant accessed or caused to be accessed Plaintiffs' and Class Members' data, communications, and personal information from California. On information and belief, Defendant uses servers located in California that allow Defendant to access and process the data, communications and personal information concerning Plaintiffs and Class Members.

170. Defendant was unjustly enriched by intercepting, acquiring, taking, or using Plaintiffs' and Class Members' data, communications, and personal information without their permission, and using it for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

171. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiffs and Class Members suffered damages.

172. Pursuant to CDAFA Section 502(e)(1), Plaintiffs and Class Members seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

173. Pursuant to CDAFA Section 502(e)(2), Plaintiffs and Class Members seek an award of reasonable attorney's fees and costs.

174. Pursuant to CDAFA Section 502(e)(4), Plaintiffs and Class Members seek punitive or exemplary damages for Defendant's willful violations of the CDAFA.

COUNT III

Use of a Pen Register or Trap and Trace Device
Cal. Penal Code § 638.51

175. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

176. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

177. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

178. Defendant's SDK constitutes a "pen register" because it is a device or process that records addressing or signaling information—Plaintiffs and Class Members' location data and personal information—from the electronic communications transmitted by their smartphones.

179. Defendant was not authorized by any court order to use a pen register to track Plaintiffs and Class Members' location data and personal information.

180. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered losses and were damaged in an amount to be determined at trial.

COUNT IV
Violation of the California Wiretapping Act
Cal. Penal Code § 631

181. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

182. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

183. The California legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, "to protect the right of privacy" of residents of California. Cal. Penal Code § 630.

184. The California legislature was motivated to enact CIPA by a concern that the "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.*

185. The California Wiretapping Act prohibits:

> any person [from using] any machine, instrument, [] contrivance, or in any other manner … [from making] any unauthorized connection, whether physically, electronically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the

> contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

186. Plaintiffs and Class Members' specific user input events and choices on their mobile devices that are tracked by Defendant's SDK communicates the user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the Wiretapping Act.

187. Plaintiffs and Class Members are residents of California, and used their smartphones within California. Accordingly, Defendant intercepts, reads, or attempts to reads Plaintiffs' and Class members' data, communications, and personal information in California.

188. On information and belief, Defendant uses servers in California to intercept, track, process, or otherwise use Plaintiffs' and Class Members' data, communications, and personal information within California.

189. Defendant intercepts Plaintiffs' and Class Members' communications while they are in transit to and from Plaintiffs' and Class Members' smartphones and the apps, app developers, and cellphone towers; Defendant transmits a copy of Plaintiffs' and Class Members' communications to itself. Defendant uses the contents of the communications to sell to third parties and in other methods for its own pecuniary gain.

190. Neither Defendant nor any other person informed Plaintiffs and Class members that Defendant was intercepting and transmitting Plaintiffs' private communications. Plaintiffs and Class Members did not know Defendant was intercepting and recording their communications, as such they could not and did not consent for their communications to be intercepted by Defendant and thereafter transmitted to others.

191. Defendant's SDK constitutes a machine, instrument, contrivance, or other manner to track and intercept Plaintiffs' and Class members' communications while they are using their smartphones.

192. Defendant uses and attempts to use or communicate the meaning of Plaintiffs' and Class Members' communications by ascertaining their personal information, including their geolocation and places that they have visited, in order to sell Plaintiffs' and Class Members' personal information to third parties.

193. At all relevant times to this complaint, Defendant intercepted and recorded components of Plaintiffs' and the putative Class's private communications and transmissions when Plaintiffs and other Class Members accessed Defendant's software via their cellular mobile access devices within the State of California.

194. At all relevant times to this complaint, Plaintiffs and other Class Members did not know Defendant was engaging in such interception and recording and therefore could not provide consent to have any part of their private and confidential communications intercepted and recorded by Defendant and thereafter transmitted to others.

195. At the inception of Defendant's illegally intercepted and stored geolocation and other personal data, Defendant never advised Plaintiffs or the other Class Members that any part of this sensitive personal data would be intercepted, recorded and transmitted to third parties.

196. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email.

197. Defendant's use of its SDK is both a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

198. At all relevant times, by using Defendant's SDK as well as tracking Plaintiffs' and Class Members' geolocation, Defendant intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and Class Members on the one hand, and the specific sites and locations Plaintiffs and Class Members visited on the other.

199. At all relevant times, by using Defendant's geolocation tracking software technology, Defendant willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and putative Class Members, while the electronic communications

were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

200. Plaintiffs and Class Members did not consent to any of Defendant's actions in implementing these wiretaps within its geolocation tracking software. Nor have Plaintiffs or Class Members consented to Defendant's intentional access, interception, reading, learning, recording, and collection of Plaintiffs and Class Members' electronic communications.

201. Plaintiffs' and the Class Members' devices of which Defendant accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

202. Defendant violated Cal. Penal Code § 631 by knowingly accessing and without permission accessing Plaintiffs and Class Members' devices in order to obtain their personal information, including their device and location data and personal communications with others, and in order for Defendant to share that data with third parties, in violation of Plaintiffs' and Class Members' reasonable expectations of privacy in their devices and data.

203. Defendant violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information and personal communications with others.

204. As a direct and proximate result of Defendant's violation of the Wiretapping Act, Plaintiffs and Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

205. Defendant was unjustly enriched by its violation of the Wiretapping Act.

206. Pursuant to California Penal Code Section 637.2, Plaintiffs and Class Members have been injured by Defendant's violation of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

COUNT V

Unfair Practices
In Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200

207. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

208. At all relevant times there was in full force and effect the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*, which prohibits, *inter alia*, "any unlawful, *unfair*, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code § 17200 (emphasis added).

209. Defendant engaged in business acts and practices which are "unfair" under the UCL, including surreptitiously collecting, tracking, using and disseminating Plaintiffs' and Class Members' personal information, geolocation data, and communications.

210. Defendant also engaged in a number of practices designed to perpetuate the scheme and the stream of revenue it generates. Those practices, which are unfair separately and particularly when taken together, include but are not limited to invasion of Plaintiffs' and Class members' privacy; surreptitiously tracking Plaintiffs' and Class members' location; surreptitiously accessing Plaintiffs' and Class Members' cellphones without authorization; surreptitiously obtaining personal data from Plaintiffs' and Class members' cellphones; surreptitiously intercepting and recording Plaintiffs' and Class Members' communications.

211. Defendant also engaged in a number of practices designed to perpetuate the scheme and the stream of revenue it generates. Those practices, which are unfair separately and particularly when taken together, include but are not limited to invasion of Plaintiffs' and Class Members' privacy; surreptitiously tracking Plaintiffs' and Class Members' location; surreptitiously accessing Plaintiffs' and Class Members' cellphones without authorization; surreptitiously obtaining personal data from Plaintiffs' and Class Members' cellphones; surreptitiously intercepting and recording Plaintiffs' and Class Members' communications.

212. Unfair acts under the UCL have been interpreted using three different tests: (1) whether the public policy which is a predicate to a consumer unfair competition action under the unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2) whether the gravity of the harm to the consumer caused by the challenged business practice outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial, not outweighed by any countervailing benefits to consumers or competition, and is an injury that

consumers themselves could not reasonably have avoided. Defendant's conduct alleged is unfair under all of these tests.

213. As a direct and proximate result of Defendant's unfair practices, Plaintiffs and Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

214. Plaintiffs seeks to enjoin further unfair acts or practices by Defendant, to obtain restitution and disgorgement of all monies generated as a result of such practices, and for all other relief allowed under California Business & Profession Code §17200.

COUNT VI
Unlawful Practices
In Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200

215. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

216. At all relevant times there was in full force and effect the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq.*, which prohibits, *inter alia*, "any *unlawful*, unfair, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code §17200 (emphasis added).

217. In the course of their business, Defendant repeatedly and regularly engaged in unlawful acts or practices that imposed a serious harm on consumers, including Plaintiffs and Class Members.

218. Defendant's acts and practices are unlawful because Defendant violated, and continues to violate:

(a) The Constitution of California, Article I, Section 1;

(b) The California Computer Data Access and Fraud Act;

(c) The California Invasion of Privacy Act; and

(d) Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

219. As a direct and proximate result of Defendant's unlawful practices, Plaintiffs and Class Members were injured and suffered damages, a loss of privacy, and loss of value of their personal information in an amount to be determined at trial.

220. Plaintiffs suffered lost money and property as a result of Defendant's violations of the UCL.

221. In using the Apps, Plaintiffs surrendered private data to Defendant that they would not have otherwise surrendered.

222. Also, there is a market for Plaintiffs' location data.

223. For more than twenty years, academics, economists, and those in the tech industry have assigned economic and monetary value to personal data.

224. Professor Paul M. Schwartz noted in the *Harvard Law Review*:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[37]

225. "Big data . . . represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[38]

226. "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[39]

227. Consumers can market and sell their own data directly, for example, through internet activity and using applications which monetize data.[40]

228. Defendant's collection and sale of Plaintiffs' data diminishes its value.

---

[37] Paul M. Schwartz, Property, Privacy and Personal Data, 117 HARV.L.REV.2055, 2056-57 (2004).

[38] *See, e.g., Supporting Investment in Knowledge Capital, Growth and Innovation, OECD,* (Oct. 13, 2013); available at: https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledgecapital-growth-and-innovation_9789264193307-en.

[39] Pauline Glickman and Nicolas Glady, *What's the Value of Your Data? TechCrunch* (Oct. 13, 2015); available at: https://techcrunch.com/2015/10/13/whats-the-value-of-your-data

[40] *See, e.g.,* Kevin Mercandante, *Ten Apps for Selling Your Data for Cash, Best Wallet Hacks* (June 10, 2020)*;* available at: *https://wallethacks.com/apps-for-selling-your-data/*;

Get Paid to Watch Ads in the Brave Web Browser; available at: https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to

229. Plaintiffs seek to enjoin further unlawful acts or practices by Defendant, to obtain restitution and disgorgement of all monies generated as a result of such practices, and for all other relief allowed under California Business & Professions Code §17200.

COUNT VII
Unjust Enrichment or Restitution

230. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

231. Plaintiffs and members of the Class conferred a benefit on Defendant through the use and dissemination of Plaintiffs' and Class Members' personal information, geolocation data, and communications.

232. Defendant received and is in possession of Plaintiffs' and Class Members' personal information, geolocation data, and communications, which Defendant used and disseminated for its own monetary benefit.

233. It is unjust under the circumstances for Defendant to retain the benefit conferred by Plaintiffs and Class members without compensating them.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order certifying the Class under Fed. R. Civ. P. 23 and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs, and the Class on all counts asserted herein;

(d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: December 19, 2024

BURSOR & FISHER, P.A.

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

AHDOOT & WOLFSON, PC
Tina Wolfson (SBN 174806)
Robert Ahdoot (SBN 172098)
Theodore Maya (SBN 223242)
Deborah De Villa (SBN 312564)
Sarper Unal (SBN 341739)
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Tel: 310.474.9111
Fax: 310.474.8585
Email: twolfson@ahdootwolfson.com
rahdoot@ahdootwolfson.com
tmaya@ahdootwolfson.com
ddevilla@ahdootwolfson.com
sunal@ahdootwolfson.com

AHDOOT & WOLFSON, PC
Melissa Clark (*pro hac vice*)
521 5th Avenue, 17th Floor
New York, NY 10175
Tel: 310.474.9111
Fax: 310.474.8585

Email: mclark@ahdootwolfson.com

Attorneys for Plaintiffs